О ТИПАХ ЕВКЛИДОВЫХ НОРМ

Г. ПОЛЛАК (Сегед)

В этой работе мы будем употреблять термин „евклидовое кольцо" в несколько более широком смысле чем обычно. Именно, мы будем говорить, что область целостности R является евклидовым кольцом, если существует отображение φ кольца R в некоторое вполне упорядоченное множество, причем

$$\varphi(ab) \geqq \varphi(b) \qquad (a, b \in R, a \neq 0) \tag{1}$$

и

$$\left\{\begin{array}{l}\text{для любых двух элементов } a, b \in R,\ a \neq 0 \text{ существует} \\ \text{такой } q \in R, \text{ что } \varphi(b - aq) < \varphi(a).\end{array}\right. \tag{2}$$

Можно предположить без ограничения общности, что φ есть отображение на некоторое беспробельное множество порядковых чисел.[1]) Так и будем поступать во всех дальнейших рассуждениях. Такое отображение будет называться евклидовой нормой, образ же элемента a при этом отображении — евклидовым образом a. Далее, два отображения φ, ψ кольца R в упорядоченные множества будем называть эквивалентными, если

$$\varphi(a) < \varphi(b) \iff \psi(a) < \psi(b).$$

Ясно, что для любого отображения φ, удовлетворяющего (1) и (2), существует единственная евклидовая норма, эквивалентная с ним.

Мы назовем типом евклидовой нормы φ кольца R порядковый тип множества порядковых чисел, на которое φ отображает R. Введение этого понятия кажется нам целесообразным потому что задавать все евклидовые нормы некоторого кольца является весьма сложной задачей даже в таком простом случае, как случай кольца целых рациональных чисел. Поэтому приходится решать сперва частные задачи. Таковой является вопрос

[1]) Множество порядковых чисел называется беспробельным, если вместе с любим своим элементом β содержит всех $\alpha < \beta$.

о всех возможных типах евклидовых норм данного кольца. В настоящей работе решим эту проблему для колец целых рациональных чисел и целых чисел комплексных полей второй степени; для колец многочленов над некоторым полем окажется возможным задать все евклидовые нормы.

Прежде чем сформулировать теорему, относящуюся к кольцу целых рациональных чисел, докажем следующую вспомогательную теорему:

Если $a_1, \ldots, a_k$ — натуральные числа и $(a_1, \ldots, a_k) = d$, то существует такое положительное число N, что при любом натуральном числе $n \geqq N$ можно представить nd в форме

$$nd = a_1 x_1 + \cdots + a_k x_k \qquad (x_i \geqq 0;\ i = 1, \ldots, k). \tag{3}$$

Достаточно доказать утверждение для $d = 1$. В этом случае всякий $n\,(>0)$ можно представить в виде

$$n = a_1 y_1 + \cdots + a_k y_k$$

с целыми $y_1, \ldots, y_k$. Представляя $y_1, \ldots, y_{k-1}$ в форме

$$y_i = x_i + a_k q_1 \quad (0 \leqq x_i \leqq a_k - 1;\ i = 1, \ldots, k-1)$$

и полагая $x_k = y_k + a_1 q_1 + \cdots + a_{k-1} q_{k-1}$, находим

$$n = a_1 x_1 + \cdots + a_k x_k.$$

Теперь надо еще позаботиться о неотрицательности x_k. Это имеет место наверняка, если

$$n \geqq a_1 x_1 + \cdots + a_{k-1} x_{k-1}$$

и тем более при

$$q \geqq (a_1 + \cdots + a_{k-1})(a_k - 1).$$

Следовательно $N = (a_1 + \cdots + a_{k-1})(a_k - 1)$ удовлетворяет выдвинутым требованиям. Тем самым вспомогательная теорема доказана[2]).

Теорема 1. Все евклидовые нормы кольца I целых рациональных чисел имеют тип $\omega \cdot \lambda$ $(1 \leqq \lambda \leqq \omega)$.

Доказательство. Пусть φ — евклидовая норма кольца I. Обозначим через d_α наибольший общий делитель всех элементов кольца I, для которых $\varphi(a) \geqq \omega \cdot \alpha$, где α некоторое порядковое число. Предположим далее, что $d_\alpha \neq 0$ и $a_1, \ldots, a_k$ — такие натуральные числа, для которых

$$(a_1, \ldots, a_k) = d_\alpha; \quad \varphi(a_i) \geqq \omega \cdot \alpha \qquad (i = 1, \ldots, k).$$

Тогда для тех $nd_\alpha \neq 0$, которые могут быть представлены из чисел a_i в форме (3), имеет место

$$\varphi(nd_\alpha) \geqq \min \varphi(a_i).$$

---

[2]) Этим простым доказательством я объязан L. Rédei.

В самом деле, пусть $nd_\alpha \neq 0$ — число, обладающее минимальным евклидовым образом среди чисел, представимых в форме (3). Тогда в (3) по меньшей мере одно из x_i отличается от нуля; пусть таковым будет например x_1. Из (2) следует, что существует $q \in I$ с

$$\varphi(a_1 + q n d_\alpha) < \varphi(n d_\alpha).$$

Но из-за $x_1 \geqq 1$ число

$$|a_1 + q n d_\alpha| = |q| n d_\alpha \pm a_1$$

тоже представимо в форме (3) и таким образом из сделанного относительно nd_α предположения следует

$$\varphi(a_1 + q n d_\alpha) = \varphi(|a_1 + q n d_\alpha|) \geqq \varphi(n d_\alpha) \quad \text{или} \quad a_1 + q n d_\alpha = 0.$$

Первый случай противоречит выбору q и поэтому невозможен. Но из-за $x_1 \geqq 1$ имеем $nd_\alpha \geqq a_1$. Поэтому второй случай может иметь место только при $nd_\alpha = a_1$. Таким образом действительно $\min \varphi(nd_\alpha) = \min \varphi(a_i)$.

Итак, если какое-либо nd_α представимо в форме (3), то $\varphi(nd_\alpha) \geqq \omega \cdot \alpha$. Так как однако в силу вспомогательной теоремы за исключением конечного числа все nd_α могут быть представлены в таком виде, то $\varphi(nd_\alpha) < \omega \cdot \alpha$ может иметь место только для конечного числа положительных n. Отсюда имеем

$$d_\beta < d_\alpha \quad \text{при} \quad \beta < \alpha,$$

так как имеется бесконечно много $a \in I$, для которых $\omega \cdot \beta \leqq \varphi(a) < \omega \cdot \alpha$, а из них только конечное число делится на d_α. Следовательно ненулевые идеалы $(d_0), (d_1), \ldots, (d_\alpha), \ldots$ образуют убывающую последовательность, а такая последовательность в кольце I не может быть длиннее чем типа ω. Поэтому φ может быть в крайнем случае типа $\omega \cdot \omega$. Но нетрудно видеть, что отображение

$$\varphi(0) = 0, \quad \varphi(\pm(2m-1)) = m, \quad \varphi(\pm 2^k (2m-1)) = \omega \cdot k + m - 1$$

$(m = 1, 2, \ldots)$ является евклидовой нормой типа $\omega \cdot \omega$. Подобным же образом могут быть легко конструированы нормы типа $\omega \cdot n$ для любого $n < \omega$, $n \neq 0$. Тем самым теорема 1 доказана.

Из комплексных полей второй степени следует рассматривать только поля с дискриминантами $\mathbf{d} = -3, -4, -7, -8, -11$, так как кольцо целых чисел будет евклидовым только в этих случаях[3]). Обозначим эти кольца последовательно через $R_1, R_2, \ldots, R_5$. Известно, что для этих R_j отображение $\varphi(a) = |a|$ обладает свойствами (1), (2), т. е. в любом классе

[3]) См. Тн. Motzkin, The euclidean algorithm, *Bulletin American Math. Soc.*, **55** (1949), 1142—1146.

вычетов $\bmod a\,(\in R_j)$ существует элемент b с

$$|b|<|a|. \tag{4}$$

Для того, чтобы стало возможным доказать теорему, подобную теореме 1, нам придется сначала выяснить, сколько таких элементов может содержаться в одном классе? Прежде всего ясно, что

$$|b-qa|<|a| \tag{5}$$

может иметь место только при

$$|q|<2, \tag{6}$$

так как в противном случае было бы из-за (4)

$$|b-qa|\geqq|qa|-|b|\geqq 2|a|-|b|>|a|.$$

В дальнейшем будем предполагать, что $b\neq 0$.

Рассмотрим теперь упомянутые кольца отдельно.

а) $j=1$ ($\mathbf{d}=-3$). Из-за условия (6) теперь возможны только случаи

$$q=0,\quad \pm 1,\quad \frac{\pm 1\pm\sqrt{-3}}{2},\quad \pm\sqrt{-3},\quad \frac{\pm 3\pm\sqrt{-3}}{2}.$$

Покажем, что в любом классе вычетов $\bmod a$ имеется по меньшей мере три элемента, удовлетворяющие (5). Введем для этой цели обозначение

$$e=\frac{1+\sqrt{-3}}{2}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}.$$

Пусть комплексное число $\frac{b}{a}$ в тригонометрической форме имеет вид

$$\frac{b}{a}=\left|\frac{b}{a}\right|\left(\cos\left(\frac{k\pi}{3}+\alpha\right)+i\sin\left(\frac{k\pi}{3}+\alpha\right)\right)\quad\left(0\leqq k\leqq 5,\ 0\leqq\alpha<\frac{\pi}{3}\right),$$

где k натуральное число. Тогда

$$|b-e^k a|=|a|\cdot\left|1-\frac{b}{e^k a}\right|=|a|\left(1-2\left|\frac{b}{a}\right|\cos\alpha+\left|\frac{b}{a}\right|^2\right)^{\frac{1}{2}}.$$

Но $\cos\alpha>\cos\frac{\pi}{3}=\frac{1}{2}$. Отсюда и из (4)

$$0<1-2\left|\frac{b}{a}\right|\cos\alpha+\left|\frac{b}{a}\right|^2<1,$$

следовательно $|b-e^k a|<|a|$. Точно так же,

$$|b-e^{k+1}a|=|a|\left(1-2\left|\frac{b}{a}\right|\cos\left(\alpha-\frac{\pi}{3}\right)+\left|\frac{b}{a}\right|^2\right)^{\frac{1}{2}}$$

и из (4) и $\cos\left(\alpha-\frac{\pi}{3}\right)\geqq\frac{1}{2}$ следует $|b-e^{k+1}a|<|a|$. Итак, $q=0$, e^k, e^{k+1} удовлетворяют (5), чем наше утверждение и доказано.

С другой стороны, если

$$\left|b-\frac{3+\sqrt{-3}}{3}a\right|<\left(\frac{2\sqrt{3}}{3}-1\right)|a|, \tag{7_1}$$

то (5) удовлетворяют $q=0$, 1, $\frac{1+\sqrt{-3}}{2}$, но для остальных возможных значений имеем

$$|b-e^k\sqrt{-3}\,a|=\left|b-\frac{3+\sqrt{-3}}{6}a+\left(\frac{3+\sqrt{-3}}{6}-e^k\sqrt{-3}\right)a\right|>$$

$$>\left(\sqrt{3}-\left|\frac{3+\sqrt{-3}}{6}\right|-\left(\frac{2\sqrt{3}}{3}-1\right)\right)|a|=|a|$$

и при $5\geqq k\geqq 2$, поскольку в этом случае аргумент комплексного числа $\sqrt{-3}\,e^{k+1}$ лежит между $-\frac{\pi}{2}$ и $\frac{\pi}{2}$, принимая кроме того во внимание, что $\frac{3+\sqrt{-3}}{6}=\frac{\sqrt{-3}}{3}e^5$, имеем

$$|b-e^k a|=\left|b-\frac{3+\sqrt{-3}}{6}a+\left(\frac{3+\sqrt{-3}}{6}-e^k\right)a\right|>\left(\frac{\sqrt{3}}{3}|e^5+\sqrt{-3}e^k|-\right.$$

$$\left.-\left(\frac{2\sqrt{3}}{3}-1\right)\right)|a|=\left(\frac{\sqrt{3}}{3}|1+\sqrt{-3}\,e^{k+1}|+1-\frac{2\sqrt{3}}{3}\right)|a|\geqq|a|,$$

т. е. в этом случае имеется точно три элемента кольца R_1, удовлетворяющие (5).

б) $j=2$ ($\mathbf{d}=-4$). Теперь возможны случаи

$$q=0,\quad \pm 1,\quad \pm i,\quad \pm 1\pm i.$$

Легко видеть, что из них подходит по меньшей мере два. В самом деле, в силу (4) подходит $q=0$; если же

$$|b\pm a|\geqq|a|,\quad |b\pm ia|\geqq|a|, \tag{8}$$

то имеем

$$|a|^2 \leqq |b \pm a|^2 = (b \pm a)(\bar{b} \pm \bar{a}) = |b|^2 + |a|^2 \pm (a\bar{b} + \bar{a}b),$$
$$|a|^2 \leqq |b \pm ia|^2 = (b \pm ia)(\bar{b} \mp i\bar{a}) = |b|^2 + |a|^2 \pm i(a\bar{b} - \bar{a}b),$$

где $\bar{a}$, $\bar{b}$ — числа, комплексно сопряженные с a, b. Отсюда

$$|b|^2 \geqq |a\bar{b} + \bar{a}b| = 2|\operatorname{Re} a\bar{b}|,$$
$$|b|^2 \geqq |i(a\bar{b} - \bar{a}b)| = 2|\operatorname{Im} a\bar{b}|$$

и сложа квадраты обоих неравенств

$$2|b|^4 \geqq 4|a\bar{b}|^2$$

или

$$|b|^2 \geqq 2|a|^2,$$

а это противоречит (4). Следовательно, из неравенств (8) по меньшей мере одно ложно, т. е. (5) выполняется каким-либо отличным от нуля q, что и требовалось.

С другой стороны, если b таково, что

$$(7_2) \qquad \left|b - \frac{a}{2}\right| < \left(\frac{\sqrt{5}}{2} - 1\right)|a|,$$

то неравенству (5) удовлетворяет только $q = 0, 1$, а для остальных возможных q получаем

$$|b + a| = \left|b - \frac{a}{2} + \frac{3}{2}a\right| \geqq \frac{3}{2}|a| - \left|b - \frac{a}{2}\right| > \left(\frac{3}{2} - \frac{\sqrt{5}}{2} + 1\right)|a| > |a|,$$

$$|b \pm ia| = \left|b - \frac{a}{2} + \left(\frac{1}{2} \pm i\right)a\right| \geqq \frac{\sqrt{5}}{2}|a| - \left|b - \frac{a}{2}\right| > |a|,$$

$$|b - i^k(1+i)a| = \left|b - \frac{a}{2} + \left(\frac{1}{2} - i^k(1+i)\right)a\right| >$$

$$> \left(\left|\frac{1}{2} + i\right| - \left(\frac{\sqrt{5}}{2} - 1\right)\right)|a| = |a|.$$

Таким образом, при выполнении условия (7_2) неравенству (5) удовлетворяют точно два элемента кольца R_2.

в) $j = 3$ ($\mathbf{d} = -7$). Возможны значения

$$q = 0,\ \pm 1,\ \frac{\pm 1 \pm \sqrt{-7}}{2}.$$

Если выполняется условие

$$(7_3) \qquad \left|b-\frac{\sqrt{-7}}{7}a\right|<\left(\frac{2\sqrt{14}}{7}-1\right)|a|,$$

то единственным подходящим значением q является 0. В самом деле, для остальных имеем

$$|b\pm a|=\left|b-\frac{\sqrt{-7}}{7}a+\left(\pm 1+\frac{\sqrt{-7}}{7}\right)a\right|\geqq\frac{2\sqrt{14}}{7}|a|-\left|b-\frac{\sqrt{-7}}{7}a\right|>|a|,$$

$$\left|b-\frac{\pm 1\pm\sqrt{-7}}{2}a\right|\geqq\left|b-\frac{\sqrt{-7}}{7}a-\frac{\pm 7+(\pm 7-2)\sqrt{-7}}{14}a\right|>$$

$$>\left(\left|\frac{7+5\sqrt{-7}}{14}\right|-\left(\frac{2\sqrt{14}}{7}-1\right)\right)|a|=|a|.$$

г) $j=4$ ($\mathbf{d}=-8$). Здесь следует рассмотреть случаи

$$q=0,\quad \pm 1,\quad \pm\sqrt{-2},\quad \pm 1\pm\sqrt{-2}.$$

Если выполняется неравенство

$$(7_4) \qquad \left|b-\frac{\sqrt{-2}}{4}a\right|<\left(\frac{3\sqrt{2}}{4}-1\right)|a|,$$

то (5) удовлетворяет только $q=0$. Действительно, для перечисленных значений q получается

$$|b\pm a|=\left|b-\frac{\sqrt{-2}}{4}a+\left(\pm 1+\frac{\sqrt{-2}}{4}\right)a\right|\geqq\frac{3\sqrt{2}}{4}|a|-\left|b-\frac{\sqrt{-2}}{4}a\right|>|a|,$$

$$|b\pm\sqrt{-2}a|=\left|b-\frac{\sqrt{-2}}{4}a+\frac{(\pm 4+1)\sqrt{-2}}{4}a\right|\geqq$$

$$\geqq\frac{3\sqrt{2}}{4}|a|-\left|b-\frac{\sqrt{-2}}{4}a\right|>|a|,$$

$$|b+(\pm 1\pm\sqrt{-2})a|=\left|b-\frac{\sqrt{-2}}{4}a+\left(\pm 1+\frac{(\pm 4+1)\sqrt{-2}}{4}\right)a\right|>$$

$$>\left(\left|1+\frac{3\sqrt{-2}}{4}\right|-\left(\frac{3\sqrt{2}}{4}-1\right)\right)|a|>|a|.$$

д) $j=5$ ($\mathbf{d}=-11$). Теперь возможно

$$q=0,\quad \pm 1,\quad \frac{\pm 1\pm\sqrt{-11}}{2}.$$

Если

$$(7_5) \qquad \left|b-\frac{2\sqrt{-11}}{11}a\right|<\left(\frac{\sqrt{165}}{11}-1\right)|a|,$$

то опять никакое значение q кроме 0 не подходит, так как в этом случае

$$|b\pm a|=\left|b-\frac{2\sqrt{-11}}{11}a+\left(\pm 1+\frac{2\sqrt{-11}}{11}\right)a\right|\geqq$$

$$\geqq\frac{\sqrt{165}}{11}|a|-\left|b-\frac{2\sqrt{-11}}{11}a\right|>|a|,$$

$$\left|b-\frac{\pm 1\pm\sqrt{-11}}{2}a\right|=\left|b-\frac{2\sqrt{-11}}{11}a-\frac{\pm 11+(\pm 11-4)\sqrt{-11}}{22}a\right|>$$

$$>\left(\left|\frac{11+7\sqrt{-11}}{22}\right|-\left(\frac{\sqrt{165}}{11}-1\right)\right)|a|=|a|.$$

Таким образом мы нашли, что для каждого кольца $R_j\,(j=1,\ldots,5)$ можно найти элемент p_j из поля отношений кольца R_j и положительное число r_j так, что при выполнении условия

$$(7_j) \qquad |b-p_ja|<r_j|a| \qquad (b,a\in R_j)$$

неравенство (5) имеет ровно n_j решений ($n_1=3$, $n_2=2$, $n_3=n_4=n_5=1$).

Теперь уже можем перейти к формулировке и доказательству теоремы, аналогичной теореме 1.

Теорема 2. Всевозможными типами евклидовых норм (евклидовых) колец целых алгебраических чисел R_j комплексных полей 2-ой степени являются предельные числа $\lambda\leqq\omega^{n_j}$.

Доказательство. Пусть φ — евклидовая норма типа $\alpha>\omega$ кольца R_j и пусть $x_0\in R_j$ с

$$(9) \qquad \varphi(x_0)\geqq\omega.$$

Рассмотрим числа $a\in R_j$, для которых

$$(10) \qquad |a|>\frac{\sqrt{1+\mathbf{d}_j}}{2r_j}|x_0|$$

и выберем из них некоторый элемент a_j с минимальным $\varphi(a_j)$. Последнее означает, что элементы $s\in R_j$, для которых $\varphi(s)<\varphi(a_j)$, не удовлетворяют (вместо a_j) неравенству (10). Следовательно

$$(11) \qquad \varphi(s)<\varphi(a_j)\Rightarrow|s|<|a_j|.$$

Так как таких элементов s только конечное число, то

$$\varphi(a_j) < \omega. \tag{12}$$

Прежде всего заметим, что при выполнении условия (10) всегда существуют решения неравенства (7_j) во всех классах вычетов $\bmod x_0$. В самом деле, пусть y — произвольный элемент кольца R_j. Положим

$$\frac{p_j a - y}{x_0} = u_j + v_j \sqrt{\mathbf{d}_j},$$

где u_j, v_j — рациональные числа, и выберем

$$t = t' + t'' \sqrt{\mathbf{d}_j} \in R_j$$

так, чтобы было $|t' - u_j| \leqq \frac{1}{2}$, $|t'' - v_j| \leqq \frac{1}{2}$. Тогда

$$|t x_0 + y - p_j a| = |x_0|\,|(t' - u_j) + (t'' - v_j)\sqrt{\mathbf{d}_j}| \leqq |x_0| \frac{\sqrt{1 + \mathbf{d}_j}}{2} < r_j |a|.$$

Если теперь $j \geqq 3$, то при надлежащем выборе t имеем

$$\varphi(t x_0 - q a_j) \geqq \varphi(a_j)$$

для всех $q \in R_j$. Действительно, для $q = 0$ это следует из (9), (1) и (12), а для остальных q из того, что, как было только что замечено, при $a = a_j$ можно найти такой $t x_0 \in R_j$, что $t x_0$ является решением неравенства (7_j). Но это противоречит тому, что φ является евклидовой нормой. Это и доказывает теорему для $j \geqq 3$.

В оставшейся части доказательства нам понадобится следующая

Лемма. Пусть R — евклидовое кольцо, φ — евклидовая норма в нем и $c \in R$, $c \neq 0$. Тогда отображение

$$\psi(a) = \varphi(ac) \qquad (a \in R)$$

удовлетворяет условиям (1), (2).

В самом деле, при $a \neq 0$

$$\psi(ab) = \varphi(abc) \geqq \varphi(bc) = \psi(b).$$

Далее, в силу (2) существует такой $q \in R$, что

$$\varphi(bc - acq) < \varphi(ac)$$

или, что то же самое,

$$\psi(b - aq) < \psi(a).$$

Тем самым лемма доказана.

Теперь рассмотрим случай $j=2$. Обозначим через d_λ наибольший общий делитель всех $x \in R_2$, для которых $\varphi(x) \geqq \omega \cdot \lambda$. Предположим, что евклидовая норма φ типа $\alpha > \omega^n j = \omega \cdot \omega$. Тогда существует неотрицательное целое число n, для которого $d_n = d_{n+1}$, так как в R_2, как и в I (и вообще в любом кольце целых алгебраических чисел), тип убывающей последовательности ненулевых идеалов не может быть свыше ω. Достаточно рассмотреть случай $n=0$, $d_n = 1$. Действительно, если для какого-нибудь $n>0$ имеет место $d_n = d_{n+1}$, то вместо φ будем рассматривать евклидовую норму χ, эквивалентную с отображением $\psi(a) = \varphi(a d_n)$. Обозначая через d'_λ наибольший общий делитель всех $x \in R_2$, для которых $\chi(x) \geqq \omega \cdot \lambda$, будем иметь очевидно

$$d'_1 = d'_0 = 1.$$

Итак, достаточно показать невозможность равенства

$$d_1 = 1. \tag{13}$$

Предположим сначала, что существуют $x_1, x_2 \in R_2$ с

$$\varphi(x_1) \geqq \omega, \quad \varphi(x_2) \geqq \omega, \quad (x_1, x_2) = 1.$$

В качестве x_0 выберем элемент $x_1 x_2$. Тогда (в силу замечания, сделанного в начале доказательства) в классе вычетов $x \bmod x_3$, определенном соотношениями

$$x \equiv 0 \pmod{x_1}, \quad x \equiv a_2 \pmod{x_2}$$

существует элемент $t_1 x_1$, являющийся (в случае $a = a_2$) решением неравенства (7_2). Значит, неравенство (5) при $a = a_2$, $b = t_1 x_1$ имеет только два решения: $q=0$ и $q=1$. Но

$$\varphi(t_1 x_1) \geqq \omega > \varphi(a_2), \quad \varphi(t_1 x_1 - a_2) = \varphi(t_2 x_2) \geqq \omega > \varphi(a_2),$$

а при $q \neq 0,1$

$$|t_1 x_1 - q a_2| \geqq |a_2|$$

и следовательно в силу (11) тоже

$$\varphi(t_1 x_1 - q a_2) \geqq \varphi(a_2).$$

Таким образом для φ не выполняется (2), что противоречит предположению.

Теперь рассмотрим общий случай. Если имеет место (13), то существуют такие $x_1, \ldots, x_n \in R_2$, что

$$(x_1, \ldots, x_n) = 1, \quad \varphi(x_k) \geqq \omega \qquad (k = 1, \ldots, n). \tag{14}$$

Невозможность этого мы и покажем. Для $n=2$ она уже показана; предположим, что n является наименьшим таким числом, для которого (14) возможно. Тогда $n \geqq 3$. Пусть

$$(x_1, \ldots, x_{n-1}) = d.$$

Тогда кольцо R_2 имеет не более чем конечное число таких элементов r, для которых

$$\varphi(rd) < \omega.$$

В самом деле, если бы их было бесконечно много, то их евклидовые образы тоже образовали бы бесконечное множество, так как нетрудно видеть, что (при данной норме) каждое натуральное число может служить евклидовым образом только конечного числа элементов R_2. Но тогда для евклидовой нормы χ, эквивалентной отображению

$$\psi(r) = \varphi(rd)$$

мы имели бы

$$\left(\frac{x_1}{d}, \ldots, \frac{x_{n-1}}{d}\right) = 1, \quad \chi\left(\frac{x_k}{d}\right) \geqq \omega \quad (k = 1, \ldots, n-1),$$

вопреки индукционному предположению. Поэтому и вследствие (14) можно выбрать такой r, что

$$\varphi(rd) \geqq \omega, \quad (rd, x_n) = 1.$$

Тем самым мы свели общий случай к случаю $n = 2$, уже опровергнутому.

Остается случай $j = 1$. Прежде всего покажем, что если $x_1, \ldots, x_n \in R_1$ и

$$\varphi(x_k) \geqq \omega \qquad (k = 1, \ldots, n), \tag{15}$$

то можно найти такие $c_1, c_1' \in R_1$ ($|c_1|, |c_1'| > 1$), что

$$c_1 | x_k \quad \text{или} \quad c_1' | x_k \qquad (k = 1, \ldots, n). \tag{16}$$

Если $|(x_1, \ldots, x_n)| > 1$, то $c_1 = c_1' = (x_1, \ldots, x_n)$ удовлетворяет (16). Поэтому можем принять $(x_1, \ldots, x_n) = 1$.

Доказательство поведем по индукции. Сначала пусть $n = 3$ (при $n \leqq 2$ утверждение тривиально). В этом случае (16) означает, что x_1, x_2, x_3 не могут быть попарно взаимно просты. Предположим, что напротив,

$$(x_1, x_2) = (x_1, x_3) = (x_2, x_3) = 1.$$

Положим $x_0 = x_1 x_2 x_3$. Тогда в классе вычетов $x \bmod x_0$, определенном соотношениями

$$x \equiv 0 \pmod{x_1}, \quad x \equiv a_1 \pmod{x_2}, \quad x \equiv e a_1 \pmod{x_3},$$

существует элемент $t_1 x_1$, являющийся решением неравенства (7_1) при $a = a_1$. Но тогда из (15), (1) и (12) получаем

$$\varphi(t_1 x_1) > \varphi(a_1),$$

$$\varphi(t_1 x_1 - a_1) = \varphi(t_2 x_2) > \varphi(a_1),$$

$$\varphi(t_1 x_1 - e a_1) = \varphi(t_3 x_3) > \varphi(a_1).$$

Далее, так как неравенство (5) при $b = t_1 x_1$, $a = a_1$ не имеет решений кроме $q = 0, 1, e$, то в силу (11) для остальных q имеем тоже

$$\varphi(t_1 x_1 - q a_1) \geqq \varphi(a_1).$$

Однако это противоречит (2) и следовательно для $n = 3$ действительно должно иметь место (16).

Переходим теперь к случаю $n \geqq 4$ и предположим, что упомянутые c_1, c_1' существуют при $m < n$ вместо n, но для n таких уже нет. Обозначим через k число простых множителей элемента $x_1 \dots x_n$ (принимая во внимание кратности). Если $k = n$, это значит, что элементы x_i — простые, но тогда любые три из них попарно просты, а это, как было доказано выше, невозможно. Поэтому предположим, что $k > n$ и при меньшем числе простых множителей искомые c_1, c_1' уже существуют, но для k уже нет таких.

Пусть c, c', c'' попарно взаимно простые элементы кольца R_1, для которых

$$|c| > 1, \quad |c'| > 1, \quad |c''| > 1,$$

$$c \, x_{m_0}, \quad c' | x_{m_1}, \quad c'' | x_{m_2} \qquad (m_p \neq m_q \text{ для } p \neq q).$$

Такие элементы существуют, так как было предположено, что для $x_1, \dots, x_n$ (16) не имеет места. Пусть например $m_0 = 1$.

Рассмотрим евклидовую норму χ, эквивалентную с отображением $\psi(a) = \varphi(ac)$. Ясно, что для элементов $\frac{x_1}{c}, x_2, \dots, x_n$ тоже не может иметь места (16) и так как число простых множетелей элемента $\frac{x_1}{c} x_2 \dots x_n$ меньше k, то (согласно индукционному предположению относительно k) имеет место хотя бы одно из неравенств

$$\chi\left(\frac{x_1}{c}\right) < \omega, \quad \chi(x_2) < \omega, \dots, \chi(x_n) < \omega.$$

Иными словами, множество элементов x, удовлетворяющих системе неравенств

$$\chi(x) < \chi\left(\frac{x_1}{c}\right), \quad \chi(x) < \chi(x_2), \dots, \chi(x) < \chi(x_n),$$

конечно. Но так как эта система эквивалентна системе

$$\varphi(xc) < \varphi(x_1), \quad \varphi(xc) < \varphi(x_2 c), \dots, \varphi(xc) < \varphi(x_n c),$$

то (из-за (15)) неравенство

$$\varphi(xc) < \omega \tag{17}$$

тоже не может иметь более чем конечное число решений. Это остается в

силе, если заменить в (17) c через c' или c'' (приведенные рассуждения могут быть повторены дословно). Поэтому можно найти такие элементы t, t', t', для которых

$$\varphi(tc) \geqq \omega, \quad \varphi(t'c') \geqq \omega, \quad \varphi(t''c'') \geqq \omega$$

и $tc, t'c', t''c''$ попарно взаимно просты. Это однако, как было доказано выше, невозможно. Тем самым доказано существование c_1, c_1', удовлетворяющих (16).

Легко видеть, что существуют также элементы c_1, c_1', удовлетворяющие условию

$$\varphi(x) \geqq \omega \Rightarrow c_1 | x \quad \text{или} \quad c_1' | x \qquad (|c_1|, |c_1'| > 1). \tag{18}$$

Действительно, рассмотрим конечное подмножество H кольца R_1, удовлетворяющее (15) и совокупность всех двоек c_1, c_1', удовлетворяющих (вместе с H) условию (16). Таких двоек имеется только конечное число. Если теперь заменяем H через $H' (\supset H)$, которое тоже удовлетворяет (15), то число подходящих двоек не возрастает. Повторяя это расширение H и соответствующее сужение множества двоек, после конечного числа шагов мы приходим к одной или нескольким парам, удовлетворяющим (16) при любом конечном подмножестве H. Ясно, что эти пары удовлетворяют также (18).

Покажем теперь, что для любого порядкового числа β, для которого $\omega \cdot \beta < \alpha$, можно найти такие элементы $c_{\beta+1}, c_{\beta+1}'$, что

$$\varphi(x) \geqq \omega \cdot \beta + \omega \Rightarrow c_{\beta+1} d_\beta | x \quad \text{или} \quad c_{\beta+1}' d_\beta | x \qquad (|c_{\beta+1}|, |c_{\beta+1}'| > 1). \tag{19}$$

Для этой цели рассмотрим опять евклидову норму χ, эквивалентную отображению $\psi(a) = \varphi(d_\beta a)$. Из определения d_β ясно, что

$$\varphi(x) \geqq \omega \cdot \beta + \omega \Rightarrow \chi\left(\frac{x}{d_\beta}\right) \geqq \omega.$$

С другой стороны, согласно уже доказанному существуют такие c, c', которые удовлетворяют (18) относительно евклидовой нормы χ. Эти же елементы удовлетворяют очевидно и (19).

В качестве следующего шага покажем, что

$$|d_\omega| > 1. \tag{20}$$

Предположим, что напротив,

$$d_\omega = 1. \tag{21}$$

Во всяком случае существуют такие элементы c_ω, c_ω', что

$$\varphi(x) \geqq \omega \cdot \omega \Rightarrow c_\omega | x \quad \text{или} \quad c_\omega' | x \qquad (|c_\omega|, |c_\omega'| > 1) \tag{22}$$

(таковы например $c_\omega = c_1, c_\omega' = c_1'$). Далее очевидно, что таких пар только

конечное число, ведь согласно (21) существуют такие элементы $x_1, \ldots, x_n$, что

$$(x_1, \ldots, x_n) = 1, \quad \varphi(x_m) \geqq \omega \cdot \omega \qquad (m = 1, \ldots, n)$$

и как c_ω, так и c'_ω должны быть делителями числа $x_1 \ldots x_n$. Обозначим через P произведение всех элементов $c_\omega \cdot c'_\omega$ и предположим, что в случае, когда P имеет меньше простых делителей, имеет место (20); покажем, что тогда это верно и при данном P. По определению $P \neq 1$; пусть $p|P$ ($|p| > 1$, p простое в R_1) и рассмотрим евклидовую норму χ, эквивалентную с отображением $\psi(a) = \varphi(ap)$. Обозначим через $\tilde{P}$ произведение всех таких элементов $\tilde{c}_\omega \cdot \tilde{c}'_\omega$, которые удовлетворяют условию

$$\chi(y) \geqq \omega \cdot \omega \Rightarrow \tilde{c}_\omega | y \quad \text{или} \quad \tilde{c}'_\omega | y \qquad (|\tilde{c}_\omega|, |\tilde{c}'_\omega| > 1). \tag{23}$$

Покажем, что существует такой y, для которого

$$\varphi(yp) \geqq \omega \cdot \omega, \quad \chi(y) < \omega \cdot \omega. \tag{24}$$

В самом деле, если из $\varphi(yp) \geqq \omega \cdot \omega$ следует $\chi(y) \geqq \omega \cdot \omega$, то тем более

$$\varphi(y) \geqq \omega \cdot \omega \Rightarrow \chi(y) \geqq \omega \cdot \omega.$$

Отсюда вытекает, что пара $\tilde{c}_\omega, \tilde{c}'_\omega$ вместе с (23) удовлетворяет также (22), т. е. $\tilde{P}|P$. С другой стороны пусть c_ω, c'_ω удовлетворяют (22), $p|c_\omega$, но pc_ω, c'_ω уже ие удовлетворяют (22). Тогда существует такой $z \in R_1$, для которого

$$\varphi(z) \geqq \omega \cdot \omega, \quad pc_\omega \nmid z, \quad c'_\omega \nmid z.$$

Из последнего следует, что $c_\omega | z$, следовательно и $p|z$. Но тогда в силу предположения относительно неверности (24)

$$\chi\left(\frac{z}{p}\right) \geqq \omega \cdot \omega, \quad c_\omega \nmid \frac{z}{p}, \quad c'_\omega \nmid \frac{z}{p},$$

т. е. c_ω, c'_ω не удовлетворяют (23). Поэтому $\tilde{P}$ имеет меньше простых делителей чем P и значит, для χ уже имеет место (20). Так как для φ (20) не имеет места, то для какого-либо y (24) должно все-таки выполняться.

Отсюда следует, что порядковый тип множества всех порядковых чисел $\varphi(rp) < \omega \cdot \omega$ меньше чем $\omega \cdot \omega$. Действительно, если

$$\varphi(rp) < \omega \cdot \omega \leqq \varphi(yp),$$

то $\chi(r) < \chi(y)$ и так как отображение $\varphi(rp) \to \chi(r)$ подобное, то порядковый тип множества всех $\varphi(rp)$ не превосходит $\chi(y)$. Но это означает, что неравенствам

$$\omega \cdot m \leqq \varphi(rp) < \omega \cdot (m+1),$$

где $m = 1, 2, \ldots$, за исключением конечного числа значений m удовлетворя-

ет только конечное число различных r и следовательно это имеет место начиная с некоторого $m = m_p$. Такое m_p можно найти для всех $p|P$. Среди них есть наибольшее:

$$M = \max_p m_p$$

и если $m \geqq M$, то существует только конечное число таких элементов r, для которых выполняется

$$\omega \cdot m \leqq \varphi(r) < \omega \cdot (m+1), \quad (r, P) \neq 1. \tag{25}$$

С другой стороны ясно, что если c_m, c'_m, удовлетворяют (19) при $\beta = m-1$, то $c_\omega = c_m$, $c'_\omega = c'_m$ удовлетворяют (22), следовательно $c_m \cdot c'_m | P$, в противоречие сказанному о (25). Тем самым доказано (20).

Наконец, докажем, что

$$|d_{\omega\cdot(n+1)}| > |d_{\omega\cdot n}|,$$

где n — произвольное натуральное число и $d_{\omega\cdot(n+1)}$ имеет смысл.

В самом деле, рассмотрим опять евклидовую норму χ, эквивалентную с отображением $\psi(a) = \varphi(a d_{\omega\cdot n})$. Так как (по определению $d_{\omega\cdot n}$) порядковый тип множества всех порядковых чисел $\chi\left(\frac{x}{d_{\omega\cdot n}}\right)$, где $\omega\cdot\omega\cdot n \leqq \varphi(x) < \omega\cdot\omega\cdot(n+1)$, равен $\omega\cdot\omega$, то

$$\varphi(y) \geqq \omega\cdot\omega\cdot(n+1) \Rightarrow \chi\left(\frac{y}{d_{\omega\cdot n}}\right) \geqq \omega\cdot\omega.$$

Поэтому применяя (20) к евклидовой норме χ получим, что все эти $\frac{y}{d_{\omega\cdot n}}$ не могут быть взаимно просты. Обозначая их наибольший общий делитель через c, получим

$$|d_{\omega\cdot(n+1)}| = |c d_{\omega\cdot n}| > |d_{\omega\cdot n}|,$$

что и требовалось.

Таким образом, последовательность идеалов (d_ω), $(d_{\omega\cdot 2})$, ... монотонно убывает, следовательно пересечение всех его членов равно нулевому идеалу. Итак, тип евклидовой нормы φ не может превзойти $\omega\cdot\omega\cdot\omega$.

Для кольца R_2 евклидовые нормы типа $\omega\cdot\omega$ и $\omega\cdot n$ $(n > 1)$ могут быть конструированы точно так же, как для I. Для R_1 отображение, определенное соотношениями

$$\psi(0) = 0,$$

$$\psi(a) = \omega^2\cdot n + \omega\cdot m + |b|^2, \quad \text{если} \quad a = 2^n(\sqrt{-3})^m b, \quad (b, 2) = (b, \sqrt{-3}) = 1$$

обладает свойствами (1), (2). Легко видеть, что эквивалентная с ψ евклидо-

вая норма имеет тип ω^3. Подобным же образом можно конструировать евклидовые нормы меньшего типа. Этим доказательство теоремы 2 завершено.

Прежде чем перейти к вопросу о кольцах многочленов, заметим, что в определении евклидового кольца условие (1) можно заменить условием

(26) $\varphi(a) = \varphi(a')$ для ассоциированных a, a'.

Действительно, пусть выполняется (26) и пусть $\varphi(ab)$ минимально среди всех $\varphi(ax)$ $(x \neq 0)$. Тогда в силу (2) существует такой q, что

$$\varphi(a - abq) = \varphi(a(1-bq)) < \varphi(ab),$$

но из-за выбора b это возможно только тогда, когда $1 - bq = 0$, т. е. когда ab ассоциировано с a. Это значит, что

$$\min \varphi(ax) = \varphi(ab) = \varphi(a).$$

Следовательно, из (26) вытекает (1). Обратное общеизвестно [4]).

Теорема 3. Отображение φ кольца многочленов $K[x]$ над полем K удовлетворяет (2) тогда и только тогда, если $\varphi(0) < \varphi(f)$ для $f \neq 0$ и

$$\operatorname{Grad} f < \operatorname{Grad} g \Rightarrow \varphi(f) < \varphi(g).$$

Следствие. Если K бесконечно мощности $\mathfrak{k}$, то всевозможными типами евклидовых норм кольца $K[x]$ являются все конфинальные с ω порядковые числа, мощность которых не превосходит $\mathfrak{k}$. Если же K конечно, то все евклидовые нормы кольца $K[x]$ типа ω.

Доказательство. Если для φ выполняются условия теоремы, то выполнение (2) для случая, когда a константа, тривиально, а когда a многочлен степени $n \geqq 1$, оно следует из того, что среди всех $f \in K[x]$ с $\varphi(f) < \varphi(a)$ находятся все многочлены меньшей степени и последние образуют полную систему вычетов $\bmod a$.

Наоборот, пусть φ обладает свойством (2). Тогда $\varphi(0) < \varphi(f)$ для $f \neq 0$ тривально. Далее, пусть $f, g_0 \in K[x]$, $\operatorname{Grad} f < \operatorname{Grad} g_0$ и g_0 таково, что его евклидовый образ минимален среди евклидовых образов многочленов g с $\operatorname{Grad} g > \operatorname{Grad} f$. Вследствие (2) существует $q \in K[x]$, для которого имеем

(27) $$\varphi(f - g_0 q) < \varphi(g_0).$$

Если бы $q \neq 0$, то имели бы

$$\operatorname{Grad}(f - g_0 q) \geqq \operatorname{Grad} g_0 > \operatorname{Grad} f$$

[4]) Существование единицы мы предположили только ради простоты. Его можно было бы вывести из (2).

и следовательно из-за выбора g_0 не могло бы иметь место (27). Поэтому $q=0$ и (27) принимает вид $\varphi(f)<\varphi(g_0)$, что и доказывает теорему.

В силу теоремы каждую евклидовую норму кольца $K[x]$ можно получить следующим образом. Множество многочленов степени n (для каждого $n \geqq 0$) разобьем на классы так, чтобы ассоциированные попали в один и тот же класс, а 0 образовал отдельный класс. Множество полученных таким образом классов упорядочим вполне, причем так, чтобы первым элементом был класс $\{0\}$, и классы, состоящие из многочленов меньшей степени, опередили классов, состоящих из многочленов более высокой степени. Полученное вполне упорядоченное множество отобразим монотонным отображением λ на беспробельное множество порядковых чисел. Обозначая через F класс, содержащий многочлен f, отображение

$$\varphi(f)=\lambda(F)$$

будет евклидовой нормой и если проделать все возможные классификации и упорядочения, то таким путем получим все различные евклидовые нормы.

Для доказательства следствия воспользуемся этой конструкцией. Обозначим через C_n упорядоченное множество классов, образованных из многочленов степени n, через γ_n его порядковый тип и через γ тип евклидовой нормы φ. Так как, очевидно, $\gamma_0=2$, то

$$\gamma=2+\gamma_1+\gamma_2+\cdots. \tag{28}$$

В случае конечного K все γ_n конечны, следовательно $\gamma=\omega$. Если же K бесконечно, то из (28) видно, что γ конфинально с ω (то, что его мощность не превосходит мощности K, тривиально). Наоборот, пусть K бесконечно мощности $\mathfrak{k}$ и пусть γ — произвольное порядковое число мощности не выше $\mathfrak{k}$ и конфинальное с ω. Тогда γ можно представить в форме (28). Обозначим через $\mathfrak{c}_n$ мощность, принадлежащая γ_n. Так как мощность множества C_n^* классов ассоциированных полиномов степени $n \geqq 1$ равно $\mathfrak{k}$, а $\mathfrak{c}_n \leqq \mathfrak{k}$, то множество C_n^* можно разбить в классы так, чтобы мощность множества этих классов равнялась $\mathfrak{c}_n$, а потом упорядочить их по типу γ_n, что и требовалось.

(Поступило 31/VIII 1959 г.)